MuSA
museum sector alliance

Data privacy and protection fundamentals

Theodor Panagiotakopoulos, Hellenic Open University

Co-funded by the Erasmus+ Programme of the European Union

Aim and objectives

- This presentation offers basic knowledge with regards to **data privacy and protection**.

- The **objectives** of this presentation are to:
  - define data privacy and data protection
  - explain who are the players in data protection
  - describe functional components and domains of data protection
  - discuss GDPR principles and data subjects
  - provide a strategy for an organization to implement data protection

Co-funded by the Erasmus+ Programme of the European Union

Learning outcomes

- At the end of this presentation, you will be able to:
  - Explain the main distinctions of data privacy and data protection
  - Recognize the three different types of stakeholders in data protection
  - Identify the seven data protection principles according to GDPR
  - Describe the four data security domains
  - Describe the four data protection functional components
  - Recognize the eight rights of data subjects
  - Outline five fundamental steps of a generic data protection strategy

Co-funded by the Erasmus+ Programme of the European Union

Table of contents

Co-funded by the Erasmus+ Programme of the European Union

MuSA
museum sector alliance

Data privacy and data protection definitions

Co-funded by the
Erasmus+ Programme
of the European Union

Introduction

- The terms data **privacy** and data **protection** are often used interchangeable

Source: https://medium.com

- In reality, they can have very **different meanings**, depending on the jurisdiction, industry or market sector they are applied.
- The **distinctions** between data privacy and data protection are fundamental to understanding how one complements the other.

Co-funded by the Erasmus+ Programme of the European Union

Data privacy vs data protection

- **Data privacy** is about authorized access — who has the data and who defines it
- **Data protection** is about securing data against unauthorized access
- Data protection is essentially a **technical** issue, whereas data privacy is a **legal** one.
- What's important to understand when comparing data **privacy vs.** data **protection** is that you can't ensure data privacy unless the personal data is protected by technology.

Co-funded by the Erasmus+ Programme of the European Union

What is data

- **Data** means information which
  - is being processed or is intended to be processed by computers operating automatically in response to relevant instructions
    - computer files, databases, emails, audio recording, etc.
  - is recorded as part of a "relevant filling system" or with the intention it should form part of a relevant filling system
    - e.g. structured paper records, such as medical records
  - is an accessible record
    - e.g. education, social work and local authority housing records

Co-funded by the Erasmus+ Programme of the European Union

What does processing means

- **Processing** in relation to information or data, means
  - obtaining,
  - recording or holding the information or data, or
  - carrying out any operation or set of operations on the information of data, including:
    - Organization, adaptation or alteration on the information or data
    - retrieval, consultation or use of the information or data,
    - disclosure of the information or data by transmission, dissemination or otherwise making available, or
    - alignment, combination, blocking, erasure or destruction of the information or data

Co-funded by the Erasmus+ Programme of the European Union

Sensitive personal data

- **Sensitive personal data** refers to personal data relating to
  - Racial of ethnic origin
  - Political opinions
  - Religious beliefs
  - Trade Union membership
  - Physical or mental health
  - Sex life
  - Offences or alleged offences

Source: https://www.macfro.com

Co-funded by the Erasmus+ Programme of the European Union

MuSA
museum sector alliance

Types of players in data protection

Co-funded by the
Erasmus+ Programme
of the European Union

Involved parties in data protection

- Data subject
- Data controller
- Data processor
- Data protection officer

Source: www.hfgproject.org

Co-funded by the Erasmus+ Programme of the European Union

Data subject

- The term **data subject** refers to the individual that the information relates to

- This encompasses all **natural persons**, who can be distinguished as persons with rights in regards to the processing of their personal data

Co-funded by the Erasmus+ Programme of the European Union

Data controller

- The **legal person** who determines how data will be processed and protected.
- In charge of **data processing** as a natural or legal person, public authority, agency or other body that, alone or jointly with others.
- The controller is responsible for determining the **purposes** for which the personal data is used and what **privacy protection** should be implemented.
- The controller can **appoint processors** for various tasks.

Co-funded by the Erasmus+ Programme of the European Union

Data processor

- Natural or legal persons, public authorities or other bodies and organizations that **process personal data** on behalf of the controller.
- The controller may have an **external IT provider** that determines where the data is stored and which technical controls are implemented.
- Or, the controller may pass some personal data to a **marketing agency** for targeted email campaigns.
- In summary, **any service provider** that obtains access to personal data, controlled by the other organization, is a data processor.

Co-funded by the Erasmus+ Programme of the European Union

Data protection officer

- In organizations, the DPO is a **guarantor of compliance** with the data protection regulations, without replacing the functions carried out by the supervisory authorities.
- **Required by** public companies and those that process data on a large scale or collect especially sensitive data or data that is related to criminal convictions or offenses
- Their **functions** include
  - supervising implementation and application of internal policies
  - staff training
  - organization and coordination of audits
  - management of interested parties' information and their request as to the exercise of their rights

Co-funded by the Erasmus+ Programme of the European Union

MuSA
museum sector alliance

GDPR principles

Co-funded by the
Erasmus+ Programme
of the European Union

Data protection principles based on GDPR

- Based on GDPR **personal data shall be**:
  1. Processed lawfully, fairly and transparently
  2. Used for specified, explicit and legitimate purposes
  3. Adequate, relevant and limited to what is necessary
  4. Accurate and kept up to date
  5. Held for no longer than is necessary
  6. Processed in a manner that ensures appropriate security
  7. Compliant with the other GDPR principles

Co-funded by the Erasmus+ Programme of the European Union

1st principle: Processed lawfully, fairly and transparently (1/2)

- The following are important to be **explicitly stated**:
  - Data controller's identity
  - The purpose for which the data are intended to be processed - what reasonable expectations the data subject had about how their data would be used?
  - In specific circumstances, any further information which is necessary to make the processing generally fair.
    - e.g. if you are going to use personal data for direct marketing you must inform the data subject

- **Must NOT deceive or mislead**

Co-funded by the Erasmus+ Programme of the European Union

1st principle: Processed lawfully, fairly and transparently (2/2)

- The data controller must be able to **justify the processing of the data** in order for that processing to be considered lawful.
- In order to be **lawful**, the **processing** must either be:
  - as a result of consent given by the data subject
  - for the performance of a contract with the individual; or
  - to comply with a legal obligation; or
  - to protect the vital interests of the individual; or
  - for the administration of justice, or the exercise of any statutory function; or
  - for the legitimate interests of the organization, unless the interests of the individual would be prejudiced

Co-funded by the Erasmus+ Programme of the European Union

2nd principle: Purpose limitation

- As a general rule, personal data must be collected only for **specified, explicit and legitimate purposes**, and used in accordance with those agreed purposes.

- The data must not be further processed in any manner **incompatible** with the original purpose for which it is collected.

Source: https://medium.com

Co-funded by the Erasmus+ Programme of the European Union

3rd principle: Data minimisation

- Personal data shall be **adequate**, **relevant** and **not excessive** in relation to the purpose or purposes for which they are processed.
- The introduction of a "**necessity**" requirement is likely to make it more difficult for data controllers to collect data for some general or as yet unspecified future use.
- Privacy notices or “how we use your information” guides now need to be **clearer than before**. This means that mere consent is not enough; the individual must be informed of exactly what their data is being used for;

Co-funded by the Erasmus+ Programme of the European Union

4th principle: Accuracy

- **Reasonable steps** must be taken to keep the information up to date and to change it if it is inaccurate.
- When an individual **updates** the information a company holds on them, the organization must stop contacting the individual using the previous details
- Organizations should be **active** in ensuring they have the correct information on an individual
- Ensure data is **not incorrect** or **misleading**
- Undertake regular **data cleansing**

Co-funded by the Erasmus+ Programme of the European Union

5th principle: Storage limitation

- Personal data processed for any purpose shall **not be kept for longer** than is necessary for that purpose.
- Organizations must **regularly review** the length of time they retain data on individuals
- Personal data **may be stored for longer periods** provided it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- This is subject to the implementation of appropriate **data security measures** designed to safeguard the rights and freedoms of data subjects.

Co-funded by the Erasmus+ Programme of the European Union

6th principle: Integrity and confidentiality

- Personal data must be processed in accordance in a manner that **ensures its appropriate security**.
- This includes **protection** against unauthorized or unlawful processing and against accidental loss, destruction or damage.
- Data controllers and processors must use appropriate technical or organizational **security measures**.

Source: https://www.information-age.com

Co-funded by the Erasmus+ Programme of the European Union

7th principle: Accountability

- The data controller is responsible for, and must be able to demonstrate, **compliance** with the other data protection principles.

- Need to put in place appropriate technical and organizational **measures** to meet the requirements of accountability, such as:
  - adopting and implementing data protection policies;
  - taking a 'data protection by design and default' approach;
  - putting written contracts in place with organizations that process personal data on your behalf;
  - maintaining documentation of your processing activities;
  - implementing appropriate security measures;

Co-funded by the Erasmus+ Programme of the European Union

MuSA
museum sector alliance

Functional components of data protection

Co-funded by the
Erasmus+ Programme
of the European Union

Information assurance

- **Information Assurance** (IA) is the study of how to protect your information assets from destruction, degradation, manipulation and exploitation. But also, how to recover should any of those happen.

- This process is **both proactive and reactive** and involves:
  - protection
  - detection
  - capability restoration
  - response

Co-funded by the Erasmus+ Programme of the European Union

Data protection functional components (1/2)

- **Protection:** ensures the availability, integrity, authenticity, confidentiality and non-repudiation of information

- **Attack detection**: the process of identifying that an intrusion has been attempted, is occurring, or has occurred

  - Intrusion is an unauthorized access to and/or activity in an information system

  - Timely attack detection and reporting is key to initiating the restoration and response processes.

Co-funded by the Erasmus+ Programme of the European Union

Data protection functional components (2/2)

- **Capability restoration**
  - Relies on established procedures and mechanisms to prioritize restoration of essential functions. Capability restoration may rely on backup or redundant links, information system components, or alternative means of information transfer.
  - A post-attack analysis should be conducted to determine the command vulnerabilities and recommended security improvements.

- **Attack response:** involves determining actors and their motives, establishing cause and complicity, and may involve appropriate action against perpetrators. It contributes by removing threats and enhancing deterrence.

Co-funded by the Erasmus+ Programme of the European Union

MuSA
museum sector alliance

Data security domains

Co-funded by the
Erasmus+ Programme
of the European Union

Data protection and security

- There are four major **domains of data protection and security**:
  - Physical security
  - Personnel security
  - IT security
  - Operational security

Source: https://www.globalsign.com

- That means that threats/risks to data protection should be considered along all four dimensions as well

Co-funded by the Erasmus+ Programme of the European Union

Data security domains (1/2)

- **Physical security** refers to the protection of hardware, software, and data against physical threats to reduce or prevent disruptions to operations and services and loss of assets.
- **Personnel security** is a variety of ongoing measures taken to reduce the likelihood and severity of accidental and intentional alteration, destruction, misappropriation, misuse, misconfiguration, unauthorized distribution, and unavailability of an organization's logical and physical assets, as the result of action or inaction by insiders and known outsiders, such as business partners.

Co-funded by the Erasmus+ Programme of the European Union

Data security domains (2/2)

- **IT security** is the inherent technical features and functions that collectively contribute to an IT infrastructure achieving and sustaining confidentiality, integrity, availability, accountability, authenticity, and reliability.

- **Operational security** involves the implementation of standard operational security procedures that define the nature and frequency of the interaction between users, systems, and system resources, the purpose of which is to
  - Achieve and sustain a known secure system state at all times, and
  - Prevent accidental or intentional theft, release, destruction, alteration, misuse, or sabotage of system resources

Co-funded by the Erasmus+ Programme of the European Union

MuSA
museum sector alliance

Data subjects' rights

Co-funded by the
Erasmus+ Programme
of the European Union

Individual rights

- The GDPR provides the following rights for individuals:
  1. The right to be informed
  2. The right of access
  3. The right to rectification
  4. The right to erasure
  5. The right to restrict processing
  6. The right to data portability
  7. The right to object
  8. Rights in relation to automated decision making and profiling

Source: https://www.coe.int

Co-funded by the Erasmus+ Programme of the European Union

Data subject's rights (1/4)

- **Right to be informed**: Data subjects have the right to be informed about the collection and use of their personal data. Privacy notices are the usual way of complying with this obligation.

Source: https://www.fphandbook.org

- **Right of access**: Data subjects have the right to be told that their data is being processed and the right to access the information held about them. Such access should be given free of charge unless the request is excessive or unfounded.

Source: https://itergy.com

Co-funded by the Erasmus+ Programme of the European Union

Data subject's rights (2/4)

- **Right to rectification**: If data held about a subject is inaccurate, the data subject can ask to have it corrected. If the organization has passed the incorrect data on to a third party, the organization should rectify with the third party too where possible.

Source: https://ico.org.uk

- **Right to erasure**: Data subjects have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

Source: https://www.readitquik.com

Co-funded by the Erasmus+ Programme of the European Union

Data subject's rights (3/4)

- **Right to restrict processing**: an individual can limit the way that an organization uses their data where they have a particular reason for wanting the restriction. This is an alternative to requesting the erasure of their data.

Source: https://activaconsulting.co.uk

- **Right to data portability**: gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format.

Source: https://www.usoft.com

Co-funded by the Erasmus+ Programme of the European Union

Data subject's rights (4/4)

- **Right to object**: object to the processing of their personal data. This effectively allows data subjects to request the termination of processing of their personal data. Applies in certain circumstances.

Source: http://www.melissasugarwrites.com

- **Right related to automated decision making including profiling**: Data subjects have the right to not be subject to automated decision-making, including profiling, which has legal or other significant effects on them.


Source: https://www.oliverwyman.com

Co-funded by the Erasmus+ Programme of the European Union

MuSA
museum sector alliance

Strategy for data protection implementation

Co-funded by the
Erasmus+ Programme
of the European Union

Data protection strategy (1/4)

- **Step 1: Learn where your data lives**
  - You can't complete your security plan until you know exactly what you're protecting and where it's stored
  - Most businesses store data on multiple media types: local disks, disk-based backup systems, offsite on tape and in the cloud. Each technology and format requires its own type of protection.
- **Step 2: Implement a need-to-know policy**
  - To minimise the risk of human error (or curiosity), create policies that limit access to particular data sets.
  - Designate access based on airtight job descriptions. Also be sure to automate access-log entries so no one who's had access to a particular data set goes undetected.

Co-funded by the Erasmus+ Programme of the European Union

Data protection strategy (2/4)

- **Step 3: Enhance network security**
  - Need to ensure network security tools (e.g. firewall and antivirus) are up-to-date and comprehensive enough to get the job done.
  - New malware definitions are released daily, and antivirus software needs to keep pace with them.
  - The bring-your-own-device philosophy is here to stay, and your IT team must extend its security umbrella over smartphones and tablets that employees use for business purposes.
  - Keep your eyes open for signs that your IT network isn't working well.
  - Duplicating data in the cloud will counter ransomware techniques.

Co-funded by the Erasmus+ Programme of the European Union

Data protection strategy (3/4)

- **Step 4: Monitor and inform your data's lifecycle**
  - Create a data lifecycle management plan to ensure the enterprise's secure destruction of old and obsolete data.
  - Identify the data you must protect, and for how long;
  - Build a multi-pronged backup strategy that includes offline and offsite tape backups;
  - Forecast the consequences of a successful attack, then guard the vulnerabilities revealed in this exercise;
  - Take paper files into account, since they can also be stolen;
  - Inventory all hardware that could possibly house old data and securely dispose of copiers, outdated voicemail systems and even old fax machines.

Co-funded by the Erasmus+ Programme of the European Union

Data protection strategy (4/4)

- **Step 5: Educate everyone**
  - Data security is ultimately about people.
  - Every employee must understand the risks and ramifications of data breaches and know how to prevent them, especially as social engineering attacks increase.
  - Talk with your employees about vulnerabilities like cleverly disguised malware web links in unsolicited email messages. Encourage them to speak up if their computers start functioning oddly.
  - Build a security culture in which everyone understands the critical value of your business data and the need for its protection.

Co-funded by the Erasmus+ Programme of the European Union

List of references

- International Association of Privacy Professionals (IAPP) Glossary
- Herrmann, D. S. (2007). Complete guide to security and privacy metrics: measuring regulatory compliance, operational resilience, and ROI. Auerbach Publications.
- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Co-funded by the Erasmus+ Programme of the European Union

Presenter's bio page

Mobile and Pervasive Computing, Quality and Ambient Intelligence Laboratory

Hellenic Open University, Patras, Greece

Email: panagiotakopoulos@eap.gr

Theodor Panagiotakopoulos was born in Greece in 1981. He received his Diploma and PhD from the Department of Electrical and Computer Engineering, University of Patras, Greece in 2006 and 2011 respectively. His research interests include, among others, pervasive computing, internet of things, ambient intelligence, mobile health and ambient assisted living systems, telemedicine and biomedical applications. Until now, he has published over 25 articles in international conferences and journals, as well as in international book chapters. He has participated in 7 National and European R&D projects focusing on IoT and e-Health, as well as on the development of educational content for digital skill acquisition in various application sectors via e-learning programs. Since 2016, he is an adjunct assistant Professor at the Department of Electrical and Computer Engineering of University of Patras.

Co-funded by the Erasmus+ Programme of the European Union

MuSA
museum sector alliance

Thank you for your attention!

Credits

- Author: Theodor Panagiotakopoulos, HOU
- Technical Reviewers: Christos Pierrakeas, HOU and Panagiota Polymeropoulou, HOU
- Scientific Reviewer: Theodor Grassos, AKMI S.A.

www.project-musa.eu

musa@daissy.eap.gr

@MuseumSectorAlliance

#MuseumSectorAlliance

Project Number: 575907-EEP-1-2016-1-EL-EPPKA2-SSA

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This presentation reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.